# Security Compliance Management

Due to the various Agencies/customers serviced by Division of Enterprise Technology (DET) and the many different laws and regulations these customers are subject to, DET must deliver secure and compliant services with common operational practices and configurations across multiple customers and jurisdictions. Given the common operational practices of the DET services, it is ultimately up to each State Agency/customer to evaluate the service offerings against their own compliance requirements to determine whether specific services satisfy their regulatory needs.

DET is committed to compliance with data protection and privacy laws generally applicable to IT service providers. Commitment is exhibited in three major areas.

- First, DET implements and maintains appropriate technical and organizational measures, internal controls, and information security practices intended to protect customer data against loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.
- Second, DET services are designed and operated with multiple safeguards utilizing industry-standard security and privacy best practices, e.g. National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls.
- Third, multiple audits are conducted annually, as independent validation, that DET complies with policies and procedures for security, privacy, continuity, and compliance.

Agencies covered by IRS Publication 1075 and/or other regulatory requirements should have their own policies, security, and training program in place to ensure their personnel do not use **DET** services in a way that violates their organizational or regulatory standards.